(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－511649
（P2000－511649A）
(43)公表日　平成12年９月５日(2000.9.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ａ	
	６４０		６４０Ｂ	

審査請求　未請求　予備審査請求　有　（全 23 頁）

(21)出願番号　特願平10－500255
(86)(22)出願日　平成８年６月５日(1996.6.5)
(85)翻訳文提出日　平成10年12月７日(1998.12.7)
(86)国際出願番号　ＰＣＴ／ＦＲ９６／００８４０
(87)国際公開番号　ＷＯ９７／４７１１０
(87)国際公開日　平成９年12月11日(1997.12.11)
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＣＮ，ＪＰ，ＵＳ

(71)出願人　ジェムプリュス　エス．セー．アー．
フランス共和国，エフ－13881　ジェムノ　セデックス，ボアット　ポスタル　100，アヴニュ　デュ　ピック　ドゥ　ベルターニュ，パルク　ダクティヴィテ　ドゥ　ジェムノ
(72)発明者　ムレイ，ダヴィッド
フランス共和国，エフ－75011　パリ，リュ　バフロア，30
(72)発明者　ナカッシュ，ダヴィッド
フランス共和国，エフ－75009　パリ，リュ　シャプタル，7
(74)代理人　弁理士　太田　恵一

(54)【発明の名称】　公開鍵暗号方法

(57)【要約】
本発明は、値G^k（ｍｏｄ）ｐを算出する離散対数に基づく公開鍵暗号方法に関するものである。本発明により、乗算回数を減らすために２つの方法が提案され、一方は、値１の少ないビット数であるがシステム全体としてのセキュリティを維持するには十分な長さの「中空の」指数ｋを生成するものであり、他方は、特定の指数について同一の内積が繰り返されることがないように指数を互いに維持しつつｇ乗する並列計算を行うものである。本発明は、デジタル署名の生成、認証および暗号化に適用される。

【特許請求の範囲】

１．　ｐはモジュールと呼ばれる素数であり、ｋはｎビットの長さにたいてい等しい乱数であり、ｇはベースと呼ばれる整数であるg^k（ｍｏｄ）ｐを算出し、エンティティＥが、かかる値を利用して別のエンティティとの間での署名を交換することを含む認証および／または署名および／または暗号化オペレーションを実現する離散対数に基づく公開鍵の暗号方法であって、

－Ｎビット長（Ｎはｎ＋ｂビットに等しい）の乱数指数値ｋを生成するステップと、

－前記指数のハミング重みＣを計算し、この値を予め固定値ｈと比較するステップと、

－乱数値kが条件：Ｃ≧ｈを満たすか否かを確認するステップと、

－このハミング重みがｈより小さい場合に乱数値ｋを拒否し、この条件を満たす指数が得られるように新たな乱数を生成するステップと、

－－方、逆の場合にはこの値を保持するステップと、

－保持した値によって式g^k（ｍｏｄ）ｐを算出するステップと、

－他のエンティティとの間で電子署名を取り交わす際にこの式を用いるステップと、エンティティについて含んでいることを特徴とする公開鍵暗号方法。

２．　満たすべき条件がｃ＝ｈであることを特徴とする請求項１に記載の方法。

３．　ｐはモジュールと呼ばれる素数であり、ｋはｎビットの長さに等しい乱数であり、ｇはベースと呼ばれる整数であるg^k（ｍｏｄ）ｐを算出し、エンティティＥが、かかる値を利用して別のエンティティとの間での署名を交換することを含む認証および／または署名および／または暗号化オペレーションを実現する離散対数に基づく公開鍵の暗号方法であって、

－以下の式

$$k_j = \Sigma a_i 2^i$$

で表される重みa_iのｎビットの乱数指数値k_jの全体を生成するステップと、

－ある指数について算出されたｇの内積が中で機能する他の指数に対して用いられるように指数と組み合わせて、$_g2^i$の内積を並列計算するステップと、

－与えられた各k_jについて、まだ計算されていない内積ｇを算出し、これらの内積を再度グループ分けして所望の式g^{k_j}（ｍｏｄ）ｐを得るステップと、

－他のエンティティとの間で電子署名を取り交わす際にかかる式を用いるステップと、

を含むことを特徴とする公開鍵暗号方法。

４．　並列計算および再グループ分けするステップが、以下のオペレーションすなわち、

－２ごとに指数を組み合わせ、それらの共通の部分を反映する指数k_cを得て、結果として得られた組み合わせを再度繰り返し、

－各k_c値について、

$G_{kc}=g^{kc}$（ｍｏｄ）ｐ

になるように値G_{kc}を計算、

－指数k_jと、前記指数が属する前記組み合わせによって得られた指数k_cとを組み合わせ、共通の部分をなくして異なる部分のみを保持し、

－与えられた指数k_jと与えられた指数k_cとの間の異なる部分を反映している指数k'_jを定義し、

値$G_{k'j}$を

$G_{k'j}=g$（ｍｏｄ）ｐ

になるように算出し、

－各繰り返し時に得られた値G_{kc}の間の乗算によって式G_{kj}（ｍｏｄ）ｐを求めることを含むことを特徴とする請求項３に記載の方法。

５．　並列計算および再グループ分けするステップが以下のオペレーションすなわち、

－指数同士を組み合わせ、共通の部分を有する指数の考えられる組み合わせのあらゆる部分集合を形成し、

－組み合わせの各部分集合について、重みのヌルではないビットが、考えられる組み合

わせの同じ重みのヌルではないビットに対応している共通の部分を反映している

指数k_cを定義し、

－各k_c値について$G_{kc}=g^{kC}$（ｍｏｄ）ｐになるように値G_{kc}を算出し、

－各指数k_jと、組み合わせの部分集合について各々得られた全ての指数k_cとを組み合わせ、指数k_jが属するこれは共通の部分をなくして異なる部分のみを保持し、

－与えられた指数k_jと与えられた指数k_c間の異なる部分を反映している指数k'_jを定義し、

－$G_{k'j}=g^{k'j}$（ｍｏｄ）ｐになるように値$G^{k'j}$を算出し、

－各k_jについて値G'_{kj}とG_{kc}との間で乗算を行うことによって式g^{kj}（ｍｏｄ）ｐを求めることを含むことを特徴とする請求項３に記載の方法。

【発明の詳細な説明】

公開鍵暗号方法

本発明は、p法値の計算を行う離散対数に基づいたいわゆる公開鍵のといわれる暗号方法を目的とするものである。

本発明は、メッセージのデジタルサインの生成，２つの単位（実体）間での認証あるいはデータの暗号化に用途がある。

このような方法において安全性は、特定の関係、とりわけ離散対数を逆にするという、そこに認められる極端な困難性に基づいている。

この問題点は、以下$y=g^x mod p$（ここで、ｙはｇｘをｐで除した余りであると定義できる）と記述する数学的関係$y=g^x p$法から考えて、ｐ、ｇおよびｙが既知である場合に、ｘを再認識することにある。この問題は、ｐのサイズが５１２ビットであるかまたはそれを越えると、かつｘのサイズが１２８ビットであるかまたはそれを越えると、現在の知識では解決することは不可能である。

このようなシステムでは、一般に、モジュールを構成している大きなサイズの番号ｐを提供する認証機関が存在する。この認証機関は、ｇによって得られる全体、すなわち数字$g^x mod p$の形成された全体のような、ベースとよばれる整数ｇも選択するが、この時ｘは間隔［０，ｐ－１］に属す、すなわち少なくとも2^{128}の最大サイズの部分集合である。

パラメータｐおよびｇはいわゆる「公開」であって、すなわち、これらは認証機関のユーザー全てに対して認証機関によって提供されるものである。

特定の変形例によれば、これらのパラメータは各ユーザーによって個別に選択され、この場合、公開鍵の完全な一部をなすものである。

暗号システムを用いる場合における主な欠点は、実行されている複雑な計算のために、比較的多くの計算および記憶手段が必要となるということにある。

事実、値$g^k mod p$の計算とは、乗算モジュールを実現することであるが、これは計

算時間およびメモリ容量においても費用がかかる。標準的なマイクロプロセッサしかを用いていない簡単な電子装置では、この種のオペレーションはほとんど実

現できない。

この種の計算専用のプロセッサを有する電子装置に関しては、それでもなお、中間値を得るのに必要な計算時間およびメモリ容量には制限するのが望ましい。

事実、値ｇｋｍｏｄｐの計算は、一般に、英語の略語ＳＱＭ（平方累乗）として知られる従来の「累乗」方法によって比較的費用のかかるものであるが、なぜならそれが平均３／２Log_2（ｐ）乗算と等しい為である。

この方法によれば、ｋがｎビット長である時ｇのすべてのべき、すなわちすべての平方：g^0、g^1、$g^2 \cdots g^n$を計算し、次に、これらのべきの間で必要な乗算を行う。（例えば、$g^{17}=g^1 \cdot g^{16}$）。

単純な「平方累乗」方法によれば、単純なg^kにもｎ／２乗算およびｎ平方が必要である。

Ｎ個の署名を一度に送信しなければならない場合には、Ｎg^kを生成し、したがって並列計算を行う。

並列「平方累乗」方法では、Ｎ×ｎ／２乗算およびｎ平方が必要である。

Ｅ．ＢＲＩＣＫＥＬＬらによって提案された、略語でＢＧＫＷと呼ばれる方法では、累乗方法を用いる場合に乗算回数を減らすことができるが、予め算出された多数の定数の記憶装置が必要があり、したがって、極めて不利益をもたらすような記憶装置のメモリー容量を備える必要がある。

この方法にＮ値の並列計算を導入することは、中間値を保持するために多数のレジスタを用いることを示している。

したがって、この方法は、極めて短い時間に多数の署名を生成することが問題となる状況にある場合には、さらに制約を生じさせるものになる。なぜならこの場合、並列計算が導入されるからである。

本発明の目的は、これらのすべての欠点を改善することにある。本発明は、すべての暗号システム、特にマイクロプロセッサのチップカードタイプの携帯式装置による、暗

号的アルゴリズムの実行のために、計算時間とメモリ容量について柔軟で費用のかからない解決策をもたらすものである。

本発明の第１の目的によれば、提案されている暗号方法は、利用されている暗号スキーム（シュノールまたはＥ１ギャマル）に従えば計算時間において１５～４０％あるいはそれ以上のゲインが得られるように、乗算モジュールの回数を減らすことを可能とする。

本発明によれば、乗算回数を減らすために２つの解決策が提案される。一つは、わずかな１ビットとともにであるが、システムのセキュリティを保護するのに十分な「中空の」指数ｋを生成することであり、他方は与えられた指数について「べき」の計算を行わないように、指数同士を組み合わせることによってべきｇの並列計算を行うことである。

本発明は、特に、値$g^k mod p$の計算を導く離散対数に基づく公開鍵暗号方法を目的としている。ここで、ｐはモジュールと呼ばれる素数であり、ｋは通常ｎビット長のランダム値であり、ｇはベースと呼ばれる整数であり、エンティティＥが認証および／または署名および／または暗号化のオペレーションを実現し、この値が介入する別のエンティティとの間での署名の交換を含むものであり、かかる暗号方法は、

－Ｎがｎ＋ｂビットに等しいＮビット長のランダム指数ｋを生成するステップと、

－この指数のハミング重みＣを計算し、この値を予め定められた値ｈと比較するステップと、

－ランダム指数値ｋがＣ≧ｈの条件を満たすか否かを確認するステップと、

－ハミング値がｈより小さい場合にランダム値ｋを除去し、この条件を満たすような指数が得られるまで新たな指数を生成することを再び開始するステップと、

－あるいは、逆の場合にはこの値を保持するステップと、

－保持した値から式$g^k mod p$を算出するステップと、

－他のエンティティとの間で電子署名を取り交わす際にかかる式を用いるステップと、

を含む。

また、本発明は、以下のような値$g^k mod$ｄの計算を導く離散対数に基づく公

開鍵暗号方法にも関するものである。ここで、ｐはモジュールと呼ばれる素数であり、ｋは通常ｎビット長のランダム値であり、ｇはベースと呼ばれる整数であり、エンティティＥが認証および／または署名および／または暗号化のオペレーションを実現し、このタイプの複数の値が介入する別のエンティティとの間での署名の交換を含み、かかる暗号方法は、

以下の式

$$k_j = \Sigma a_i 2^i$$

で表される重みa_iのｎビットのランダム指数k_jの全体を生成するステップと、

－ある指数についてすでに算出されたべきｇが、それが介入する別の指数に役立つように、指数を組み合わせて、$g 2^i$の「べき」を並列計算するステップと、

－与えられた各k_jについて、まだ計算されていないべきｇを計算し、これらのすべての「べき」を再度グループ分けして所望の式$g^{kj} \mathrm{mod} p$を得るステップと、

－他のエンティティとの間で電子署名を取り交わす際にかかる式を用いるステップと、を含む。

本発明の一実施態様によれば、並列計算および再グループ分けのステップは以下のオペレーション、

－２つごとに指数を組み合わせ、その共通部分を反映する指数ｋｃを得て、得られた組み合わせの結果について組み合わせを繰り返すステップと、

－各ｋｃ値について、

$$G_{kc} = g^{kc} \mathrm{mod} p$$

になるように値G_{kc}を計算するステップと、

－共通の部分をなくし、異なる部分のみを保持するようにこの指数が組み合わせによって得られた指数k_cを指数k_jと組み合わせるステップと、

－与えられた指数k_jと与えられた指数k_cとの間の異なる部分を反映している指数k'_jを定義し、

－値$G_{k'j}$を

$$G_{k'j} = g^{k'j} \mathrm{mod} p$$

になるように算出し、

－各繰り返し時に得られた値$G k_c$の間で乗算を行うことにより式$G_{kj} mod p$を求めるステップを含む。

本発明の第２の実施態様によれば、並列計算および再グループ分けのステップは以下のオペレーション、

－共通の部分を有する指数の可能な組み合わせの部分集合を形成するように指数を組み合わせるステップと、

－与えられた重みのヌルではないビットが、考慮対象となる組み合わせの同じ重みのヌルではないビットに対応しているような組み合わせの各部分集合について共通部分を反映している指数k_cを定義し、

－各ｋｃ値について$G_{kc} = g^{kc} mod p$になるように値G_{kc}を算出し、

－各指数k_jと、これに対してこの指数k_jが共通部分をなくして異なる部分のみを保持するように属する組み合わせの各部分集合について、各々得られた指数k_c全てを組み合わせるステップと、

－与えられた指数k_jおよび与えられた指数k_cの間の異なる部分を反映している指数k'_jを定義し、

－$G_{k'j} = g^{k'j} mod p$になるように値$G_{k'j}$を算出し、

-各k_jについて値G'_{kj}とG_{kc}との間で乗算を行うことによって式$g^{kj} mod p$を求めるステップを含む。

本発明の他の目的によれば、指数間での共通の部分を得られるようにする組み合わせは、論理和「ＡＮＤ」によって実現される。

本発明の他の目的によれば、異なる部分を得られるようにする組み合わせは、「排他

的論理和」論理関数によって達成される。

本発明の他の特徴および利点は、添付の図面を参照して説明する例示的かつ非限定的な実施例による説明を読むことで明らかになろう。

－図１は、本発明を実施するのに適したシステムを示す基本図である。

－図２は、第１の実施例における方法の主なステップを示す機能図である。

－図３は、本発明の第１の実施態様による第２の実施例における方法の主なステップを示す機能図である。

－図４は、本発明の第２の実施態様による第２の実施例における方法の主なステップを示す機能図である。

図１に、本発明の目的である暗号方法の実施システムの基本図を示す。

このシステムは、少なくとも１つの他のエンティティＥ２と電子信号を交換したいと考えているエンティティＥ１からなる。各エンティティには、中央処理装置（ＣＰＵ）１１、３０と、通信インタフェースと、揮発性メモリ（ＲＡＭ）１３、３２および／または書き込み不可メモリ（ＲＯＭ）１４、３４および／または書き込み可能なまたは再書き込み可能な不揮発性メモリ（ＥＰＲＯＭまたはＥＥＰＲＯＭ）１５、３３と、アドレスバス、データバスおよび制御バス１６、３５を備えている。

処理装置および／またはＲＯＭは、本発明の目的たる方法において、すなわち、認証セッションの時、電子署名生成時、あるいは他のエンティティに送られる電子信号の暗号化時に行われる計算ステップの実施に対応するプログラムまたは計算リソースを有している。

処理装置またはＲＯＭは、モジュールの乗算、加算および減算の実施に必要なリソースを有している。

処理装置および／またはＲＯＭは、各暗号化アルゴリズム専用に用いられる暗号機能とおよびパラメータｇおよびｐを含んでいる指数k_jは、認証機関によって再書き込み可能メモリに予め記憶させることができ、あるいは、乱数発生器または秘密乱数ソースk_oから順次生成することもできる。さらにエンティティＥ１は秘密鍵ｘを有している。

本発明は、口座上で行われるトランザクションにおいて厳格なセキュリティが必要と

される銀行分野で実施される暗号システムに特に利用される。また、他のエンティティから電子信号形式として送信されるメッセージの送信を認証したい場合にも同様である。さらに、他のエンティティとの信号の交換時にメッセージに署名

する必要がある場合も同様である。

実際、トランザクションを行いたいと思っているエンティティは、例えばチップカードなどの集積カードであり、この場合は目的地となるエンティティは銀行端末などである。

説明の後半は、本発明が離散アルゴリズムに基づく任意の暗号システムに適用できるという理解できるのでデジタルメッセージへの署名にこの方法を適用することについて述べるものである。

本発明による方法は、特にメモリ容量が少ない環境に適している、乗算回数を大幅に減らす第１の解決策を提案するものである。

この場合、原則は、指数のランダムな性質を当然維持したままで、選択されるハミング重みが可能な限り最も軽いという意味で「中空の」指数k_jを生成するということである。

この目的のために、本発明による方法は、必要に応じて順次指数k_jを生成するか、あるいは交換がなされる前に予め指数k_jを生成することにある。この場合、当然これらの指数は記憶される。生成された指数はｎビットの長さではなくｎ＋ｂビットを超える長さであり、以下において定義する条件を満たす。

ｎ＋ｂの指数ｋが生成されると、本方法は次にかかる指数のハミング重みＣを算出し、続いてこれを予め定めた値ｈと比較する。

比較結果が$C \geqq h$である場合には、指数は保持されエンティティによって利用されるが、このエンティティは、式$g^k \bmod p$を算出し、式を例えば署名として利用する様なデジタル信号を送信する際にこの式を利用する。

パラメータＣが必要な条件を満たさない場合には、対応する指数ｋは除外され、新たな指数が生成され、この条件を満たす指数ｋが得られるまで、条件についての確認ス

テップが再度実行される。

このように、この解決方法では、より小さな指数を用いた場合と全く同じセキュリティレベルを保持したままより少ない乗算を行うことを可能にするものである。

乗算回数を最大限に減らすことができる特別な実施例においては、ｃ＝ｈが選択される。

事実、ハミングの重みがｈであるn+bビット長（ｎ=$\log_2$pの場合）の指数の場合、つまりこの指数がｎビットの場合と同じ結合数を有する場合、次の関係が立証されなければならない。

$2^n \leqq {}^{ch}_{n+b}$と、

（Ｎ+ｂ）／２+ｈ≦ｎ

（実行する計算数を削減することが出来ることを条件とする。）

つまり、２ｎ≦（ｎ+ｂ）！／（ｎ+ｂ-ｈ）！ｈ！

および

ｂ+２ｈ≦ｎ

決定するｂとｈの数は与えられた1個のｎ（たとえばｎ＝160）のこの二重条件付不等式を解いて求められる。

例証として、本発明による方法の結果と既知の方法とを比較してみた。

ｎ＝160ビットのシュノールのアルゴリズムの場合と、ｎ＝512ビットのＥ１ギャマル　アルゴリズムの場合。これらの結果を下表に示す。

変数 力	シュノール	Ｅ１ギャマル 計算時間	Ｅ１ギャマル メモリ空間
乗算	６２（ｈ）	１８７（ｈ）	１９９（ｈ）
平方	８７（ｂ＝１５）	２７９（ｂ＝５２）	２７３（ｂ＝３５）
力	１４９	４６９	４７２
ゲイン	６．８％	９．４％	７．８％

ｎビットの指数によって覆われた署名空間にかかる応力を、得ることを希望するセキュリティーのレベルによりα関数によって減少させることが出来る。

よって、パラメータｎ、ｈ、ｂは条件（１）を満たす必要がある。

（１）$2^{n-a} \leqq$（ｎ＋ｂ）！／（ｎ＋ｂ－ｈ）！ｈ！

この場合、（ｎ＋ｂ）ビット長の異なる確率変数から同一の署名を発生させる可能性を有する。

事実、2^{80}は可能な様々なアタックを妨げるのに十分であり、したがってn-αを＝100は許容出来る値である。

変数 力	中空の指数 計算時間	中空の指数 メモリ空間	単純な平方累乗
乗算	３７（h）	４９（h）	n／２
平方	n／２＋７ （b＝１４）	n／２＋２ （b＝４）	n／２
合計	n／２＋４４	n／２＋５１	n

この実行変数は、平方のコスト（計算時）がモジュール乗算のコストよりも少ないためますます注目に値する。

一般には次のようになる。

計算する平方の数ｓがｓ/2≦ｍ≦ｓで、ｍが乗算の数である場合、この極端な二つケースは、ｍ＝ｓとｍ＝2ｓとなる。

この二つの極端なケースを比較した結果を下表に表す。

変数 力	中空の指数 計算時間	中空の指数 メモリ空間	単純な平方累乗	ゲイン
シュノール （m＝２ｓ）	１２４	１３１	１６０	２２．５％
EIギャマル （m＝２ｓ）	３００	３０７	５１２	４１％
シュノール （m＝ｓ）	２０４	２１１	２４０	１５％
EI ギャマル （m＝ｓ）	５５６	５６３	７２８	２４％

シュノールとEIギャマルの図表にこの手順を適用した場合に求められたゲインは、単純に乗算した乗法と比較した場合も、１次数のコストが乗算コストと同じと

考えられる場合にも、極めて大きい。

別の実施方法によると、この手順はメモリ空間に関し、特に特別な応力のないシステムに適用される。

この実施方法においては、次数の計算を一回に限るためにｇの異なるべきの並列計算を行い、同一計算を数回にわたり実行しないように、指数を結合する。

本発明をよりわかりやすくするために、２つのべきの計算方式を説明する。

$k_j = \Sigma a_i 2^i$この場合のk_jは乱数として求められた。（つまり、乱数発生器に基づき生成された）または、

$k_k = k_j = \Sigma b_i 2^i$

本手順に従って、$k_c = \Sigma a_i b_i 2^i$がk_jとk_kの間の共通部分を反映し、係数a_iが１か０となるように、指数k_cを規定するように指数k_jとk_kを結合する。

指数k_cはk_jとk_kの共有部分に該当する。つまり、

$k_j = 1\times 2^{10} + \ldots + 0 + 1\times 2^0$と、

$k_k = 1\times 2^{10} + 0 + 0 \ldots + 1\times 2^0$

$k_c = 1\times 2^{10} + 0 + \ldots + 1\times 2^0$

本手順に従って、論理関数ETによって指数kをk_cとする。

次に、指数k_jと指数k_c間の確実な部分を決定する2番目の組み合わせを行う。

同様に、指数k_kとk_c間の確実な部分も算出する。

排他的論理和として実行された組み合わせを $k_j \oplus k_c$ および $k_k \oplus k_c$ とする。

次の次数を並列計算する。

$$G_{kj} = g^{kj \oplus kc} \bmod p$$

$$G_{kk} = g^{kk \oplus kc} \bmod p$$

$$G_{kc} = g^{kc} \bmod p$$

$g^{kj} \bmod p$と$G^{kk} \bmod p$を求めるには、次の演算を実行する。

1) $G_{kj} \times Gk_c \bmod p$

2) $Gkk \times Gk_c \bmod p$

2つの累乗を与えた上記の例と同様、n乗算ではなく平均して約3n/4の乗算を実行する。ゲインは25％となる。

本発明による手順は、最大数の指数の組み合わせで広げることが出来る。このような拡大は、図3と4に示すフローチャートで説明する2つの実行方法に従い導入することが出来る。

この場合、本発明は特に大量の署名を発生させる必要のある場合に特に適用される。

第一の実行方法により、下表により表される木構造のように2つずつ指数の組み合わせを行う。

k_j	a1 ` a2	a3 a4
k_c	b1=a1・a2	b2=a3・a4
	c1=b1・b2	

この組み合わせにより、上記の例と同様、指数k_cをk_jの間の共通部分に反映させることが出来る。

簡単に記述するためには、指数k_jをa_1、a_2、a_3、a_4とする。

指数k_cをツリーの-1レベルでb_1とb_2とし、ツリーの-2レベルでc_1とする。

a_1・a_2、a_3・a_4の組み合わせを論理関数ANDにより実行する。

このように構成されているツリーの各レベルで組み合わせを反復する。ビットの単純な統計分布によりツリー内に進むにつれ乗算回数が減少する。n/3乗算により実行する計算の成果が減じられる。

上述のように、各レベルでG_{kc}の値が決定される。

この結果、次の式が得られる。

$$G_{a1} = g^{a1 \oplus b1} \bmod p$$

$$G_{a2} = g^{a2 \oplus b1} \bmod p$$

$$G_{b1} = g^{b1} \bmod p$$

$$G_{b1} = g^{b1 \oplus c1} \bmod p \text{ または } G_{b1} = G_{b1} \cdot G_{c1} \bmod p$$

$$G_{b2} = g^{b2 \oplus c1} \bmod p \text{ または } G_{b2} = G_{b2} \cdot G_{c1} \bmod p$$

$$G_{c1} = g^{c1} \bmod p$$

$$G^{a1} \bmod p = G_{a1} \times G_{b1} \bmod p = G_{a1} \times G_{c1} \bmod p$$

実際、$g^{a1} \bmod p$は$G_{a1} \times G_{b1} \bmod p$の関により求められる。また$g^{a2} \bmod p$ $G_{a2} \times G_{b1} \times G_{c1} \bmod p$の関により求められる。

第二の方法によれば、指数を可能なあらゆる組み合わせの部分集合をなすように組み合わせるが、すなわち、例えば、指数kj：a,b,cでは、ab,ac,bc,abcの組み合わせを作る。

つまり論理関数ANDをaとb、aとc,bとc,bとcとa,b,cの間に行うことにより、これらの部分集合について共通部分を定められるような組み合わせをつくる。このようにして累乗指数k_cを、各部分集合について定める。

すべての$G_{kc}=g^{kc} \bmod p$値の並列計算ができ、それらのK^cは初めのＫに対してわずかに１ビットを有し、従って、それらについてのモジュラー変換も早い。

次に、一つの指数と、上述の組み合わせとの間で共通部分をとりのぞくことからなるまた別の組み合わせをつくる。

これらの組み合わせは論理関数で行う。このようにして次が得られる。

ka=a xor abc xor ac xor ab

kb=b xor abc xor ab xor bc

kc=C xor abc xor ac xor bc

次に$G_{kj}=g^{xj} \bmod p$を求めることができ、この$k_{,j}$はさらにイニシャルk_cよりも１ビットが少なく、そのモジュラー変更速度はさらに早い。

最後に$g^{kj} \bmod p$の式がk_jによって得られる。

この第二の実施態様で得られた署名発生Ｎの場合、演算は、次のように示される。

n/N二乗+n(2^N-1)/N2^N+(2^{N-1}-1)乗算

次の表は、掛け算二乗、平行乗算二乗、および本発明のような周知の方法と比較した場合の結果を示している。

方法 効果時間	平方累乗	並列平方累乗	二分木 指数組み合わせ
二乗	N(n-1)	n-1	n-1
乗算	N(n/2-1)	N(n/2-1)	Nn/3
トータル	N(3n/2-2)	N(n/2-1) +n-1	Nn/3+n-1
N>>nについての効果	100%	33%	22%

署名Nの発生に適用される場合における与えられた第一の実施態様（木構造分類）はメモリー容量ではコストが安い。

指数４の二分木については計算に、$\log_2(p)$ビットの８つのレジスタが必要となるの

であろう。

与えられた第二の実施態様（N分類）が、計算時間において費用が非常に安いのは、乗算の回数において最適なためである。

３つの指数の場合、計算のために$\log_2(p)$ビットの８つのレジスタが必要であろう。

【図１】

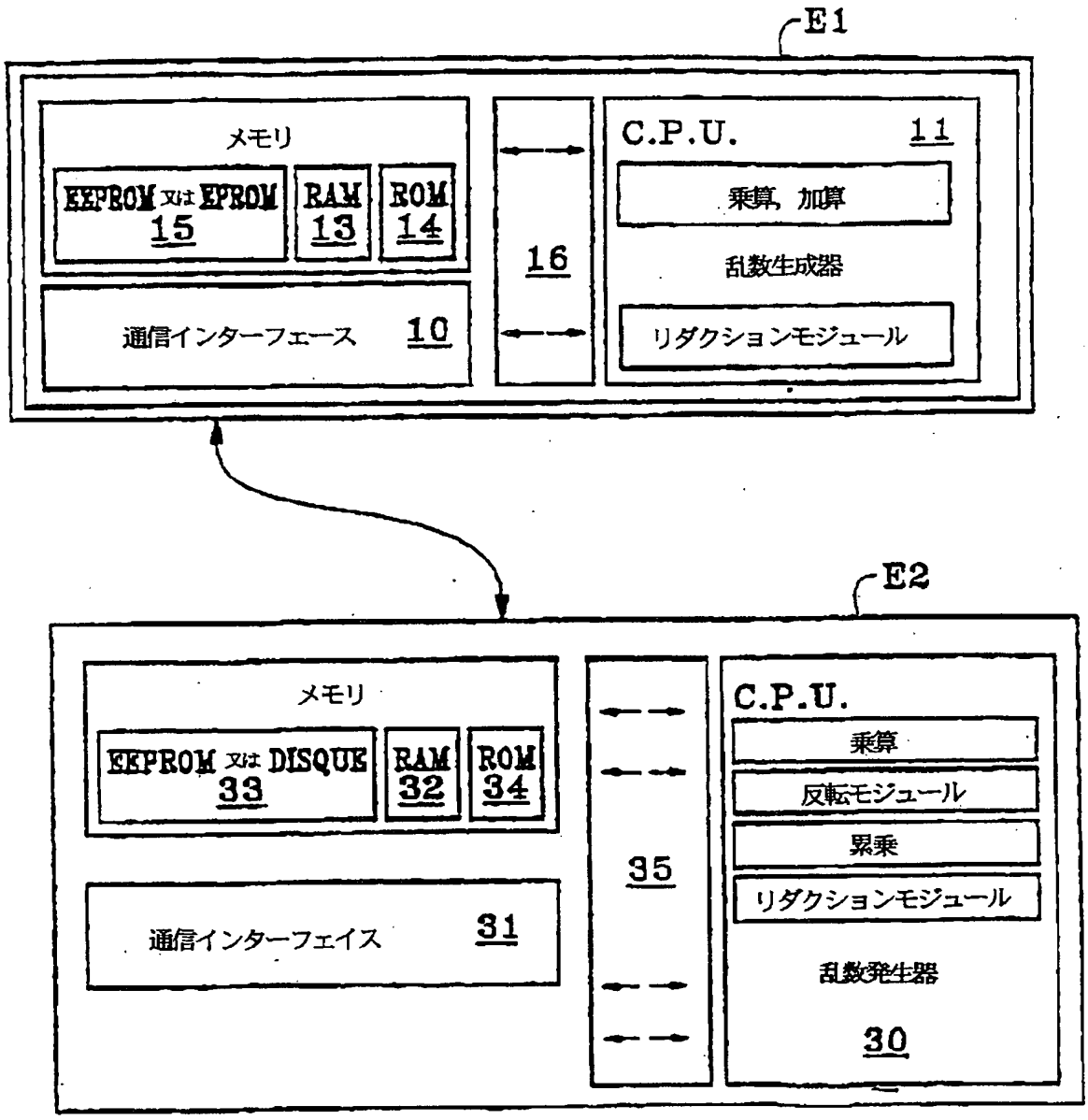
E1
メモリ
EEPROM 又は EPROM
15
RAM
13
ROM
14
通信インターフェース
10
16
C.P.U.
11
乗算, 加算
乱数生成器
リダクションモジュール
E2
メモリ
EEPROM 又は DISQUE
33
RAM
32
ROM
34
通信インターフェイス
31
35
C.P.U.
乗算
反転モジュール
累乗
リダクションモジュール
乱数発生器
30

FIG.1

【図２】

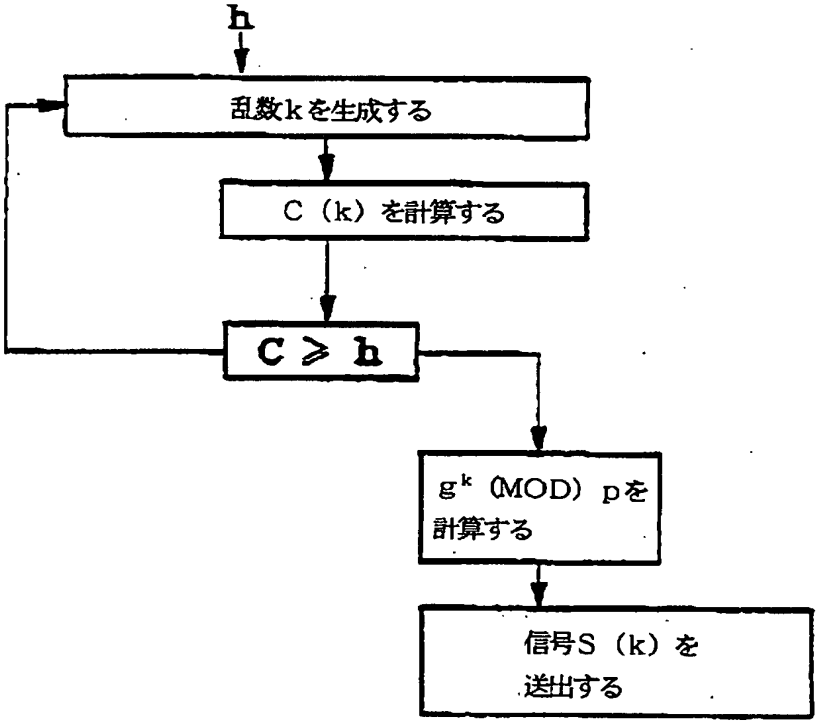

FIG.2

【図３】

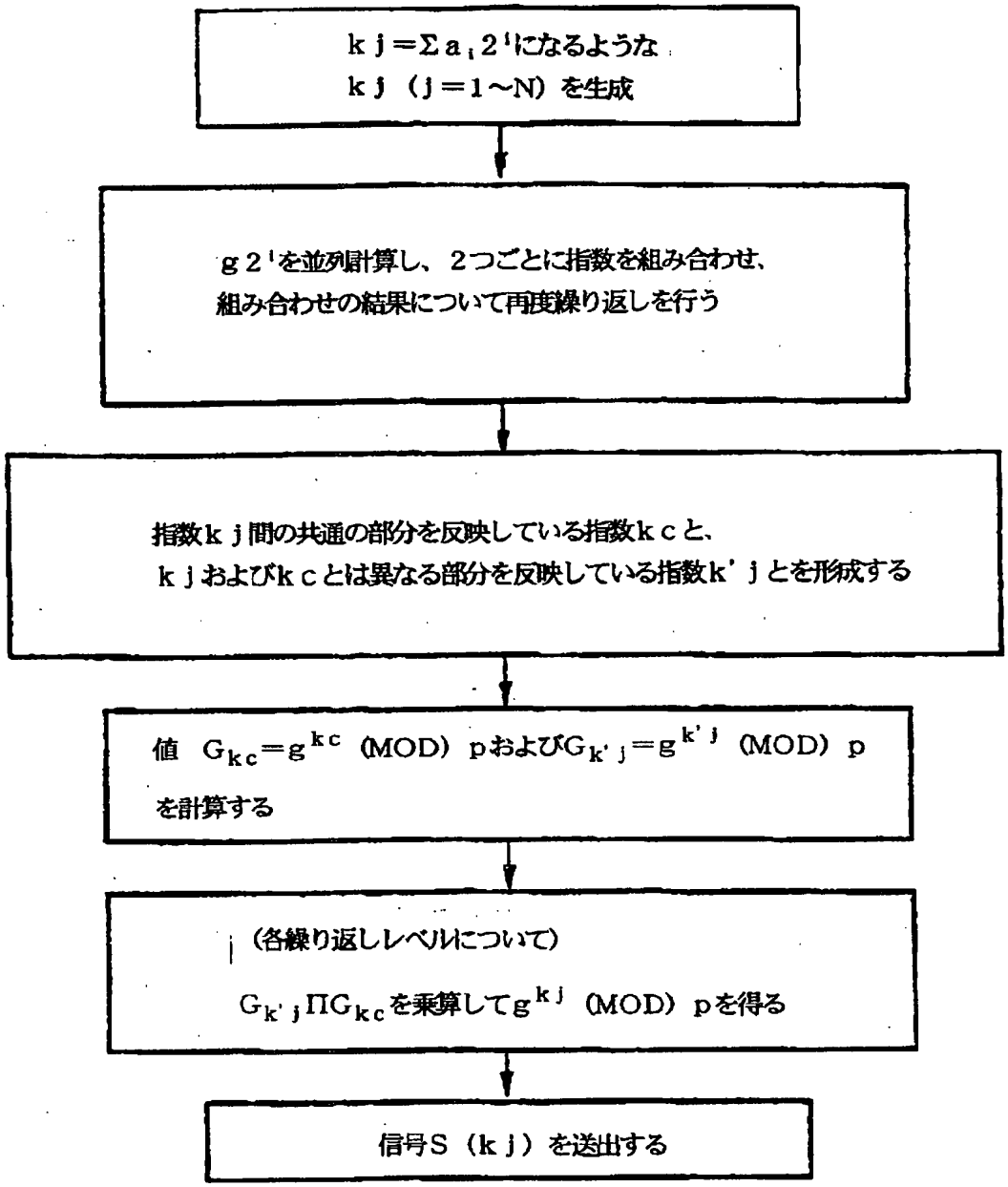
kj＝Σa_i 2^i になるような
kj （j＝1～N）を生成
g 2^i を並列計算し、２つごとに指数を組み合わせ、
組み合わせの結果について再度繰り返しを行う
指数kj間の共通の部分を反映している指数kcと、
kjおよびkcとは異なる部分を反映している指数k' jとを形成する
値 G_kc＝g^kc (MOD) pおよびG_k'j＝g^k'j (MOD) p
を計算する
(各繰り返しレベルについて)
G_k'j ΠG_kc を乗算してg^kj (MOD) pを得る
信号S（kj）を送出する

FIG.3

【図４】

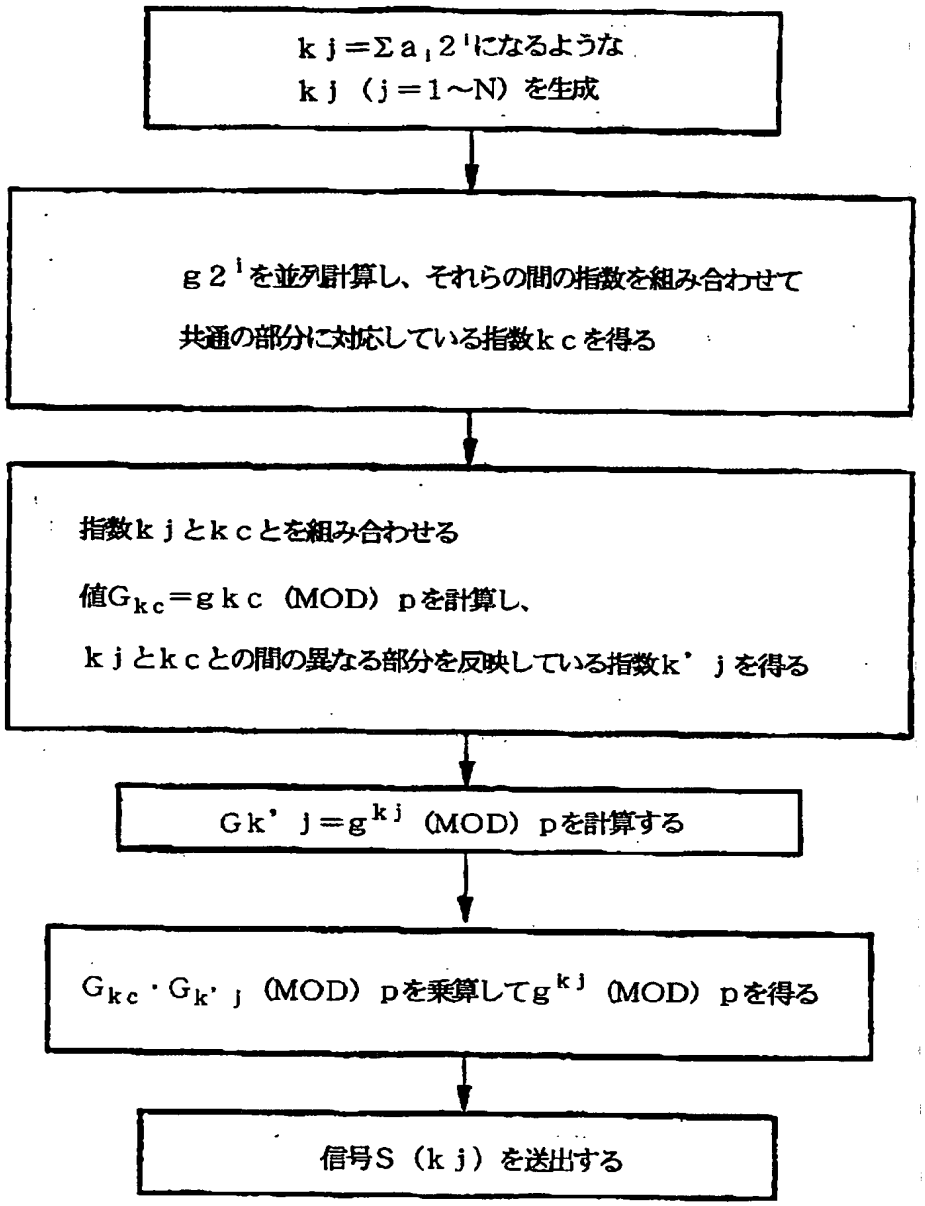
kj＝Σa_i 2^i になるような
kj（j＝1～N）を生成
g2^i を並列計算し、それらの間の指数を組み合わせて
共通の部分に対応している指数kcを得る
指数kjとkcとを組み合わせる
値G_kc＝gkc（MOD）pを計算し、
kjとkcとの間の異なる部分を反映している指数k'jを得る
Gk'j＝g^kj（MOD）pを計算する
G_kc・G_k'j（MOD）pを乗算してg^kj（MOD）pを得る
信号S（kj）を送出する

FIG.4

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna l Application No
PCT/FR 96/00840

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/30 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PROCEEDINGS OF THE IEEE 1989 CUSTOM INTEGRATED CIRCUITS CONFERENCE (CAT. NO.89CH2671-6), SAN DIEGO, CA, USA, 15-18 MAY 1989, 1989, NEW YORK, NY, USA, IEEE, USA, pages 12.3/1-5, XP000075631 ROSATI T: "A high speed data encryption processor for public key cryptography"	1
A	see page 12.3.1, right-hand column, line 1 - line 18 see page 12.3.3, right-hand column, line 12 - line 26 see page 12.3.4, left-hand column, line 15 - line 26	3
	--- -/--	

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance
'E' earlier document but published on or after the international filing date
'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
'O' document referring to an oral disclosure, use, exhibition or other means
'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 February 1997	- 4. 03. 97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna l Application No
PCT/FR 96/00840

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ELECTRONICS LETTERS. 17 AUG. 1989. STEVENAGE UK, vol. 25, no. 17, ISSN 0013-5194, pages 1171-1172, XP000054000 JEDWAB J ET AL: "Minimum weight modified signed-digit representations and fast exponentiation" see page 1171, left-hand column, last paragraph - right-hand column, line 17 see page 1171, right-hand column, line 41 - line 49 ---	1
A	ADVANCES IN CRYPTOLOGY - AUSCRYPT '92. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES PROCEEDINGS, GOLD COAST, QLD., AUSTRALIA, 13-16 DEC. 1992. ISBN 3-540-57220-1, 1993, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, pages 447-456, XP000470453 SUNG-MING YEN ET AL: "The fast cascade exponentiation algorithm and its applications on cryptography" see page 448, line 1 - page 449, line 4 -----	3

Form PCT/ISA/210 (continuation of second sheet) (July 1992)